SOLUTION BRIEF

Accesso remoto sicuro per la tua forza lavoro su vasta scala

Sintesi preliminare

Le organizzazioni sono chiamate a confrontarsi con una serie di potenziali situazioni di emergenza come malattie, alluvioni, uragani e blackout. L'introduzione di un piano di continuità operativa è essenziale per garantire che l'organizzazione sia in grado di mantenere l'operatività di fronte alle avversità e pronta ad affrontare potenziali calamità.

Una considerazione importante per le organizzazioni che sviluppano un piano di business continuity è che l'organizzazione può non essere in grado di sostenere le normali attività in sede. La capacità di supportare i dipendenti che lavorano a distanza è essenziale per garantire sia la continuità operativa che la sicurezza. Le soluzioni Fortinet offrono uno strumento integrato per supportare il telelavoro. I firewall di nuova generazione (NGFW) FortiGate integrano il supporto delle reti private virtuali (VPN) IPsec, consentendo ai lavoratori remoti di connettersi in modo sicuro alla rete aziendale. Con la protezione degli endpoint fornita da FortiClient e l'autenticazione a più fattori (MFA) garantita da FortiAuthenticator, le organizzazioni possono supportare in modo sicuro il lavoro a distanza e mantenere la continuità aziendale.

La capacità di supportare in modo sicuro la forza lavoro remota è una componente essenziale del piano di business continuity e disaster recovery di qualsiasi organizzazione. A causa di un blackout o un evento analogo, come anche di una malattia o un'alluvione che può rendere insicura la presenza dei dipendenti, un'organizzazione può non essere in grado di sostenere le normali attività in sede.

In questi scenari, un'organizzazione deve essere in grado di supportare una connettività sicura in remota alla rete aziendale. Per oltre 400.000 clienti Fortinet, la distribuzione della tecnologia esistente contiene già questa funzionalità. I firewall NGFW FortiGate integrano il supporto delle VPN IPsec, consentendo una connettività sicura per i dipendenti che lavorano da postazioni di lavoro alternative.

In media, il telelavoro riduce il tempo improduttivo dei dipendenti del 27%.[1]

I dipendenti remoti lavorano in media 16,8 giorni in più all'anno rispetto ai dipendenti in sede.[2]

L'85% dei dipendenti dichiara di raggiungere la massima produttività quando telelavora.[3]

Consentire il telelavoro ha aumentato la retention dei dipendenti nel 95% delle organizzazioni.[4]

Garantire la sicurezza della forza lavoro remota con i firewall NGFW FortiGate

Le VPN IPsec e SSL integrate in ogni firewall NGFW FortiGate offrono un modello estremamente flessibile di distribuzione. I lavoratori remoti possono trarre vantaggio da un'esperienza senza client o accedere a funzionalità aggiuntive attraverso un client di spessore integrato nella soluzione di sicurezza per endpoint FortiClient. I power user e i super user trarrebbero vantaggio dalla distribuzione di un FortiAP o un firewall NGFW FortiGate per ulteriori funzionalità.

Le soluzioni Fortinet sono progettate per essere facili da usare dall'acquisto iniziale sino alla fine del ciclo di vita. I firewall NGFW FortiGate e i gli access point wireless FortiAP includono la funzionalità di distribuzione zero-touch. Gli apparecchi distribuiti in postazioni remote possono essere preconfigurati prima della spedizione, il che ne consente la configurazione automatica in loco, garantendo così la continuità operativa e supportando il telelavoro.

Il Fortinet Security Fabric sfrutta un sistema operativo Fortinet comune e un ambiente API (Application Programming Interface) aperto per creare un'architettura di sicurezza ampia, integrata e automatizzata. Grazie al Fortinet Security Fabric, tutti i dispositivi di un'organizzazione, compresi quelli distribuiti in remoto per supportare il telelavoro, possono essere monitorati e gestiti da un'unica interfaccia. Da un firewall NGFW FortiGate o una piattaforma di gestione centralizzata FortiManager distribuita nell'ambiente della sede centrale, il team di sicurezza può ottenere la piena visibilità di tutti i dispositivi collegati, indipendentemente dalla loro situazione di distribuzione.

In caso di calamità naturale o altro evento che blocchi le normali attività aziendali, un'organizzazione deve essere in grado di passare rapidamente a una forza lavoro completamente remota. La tabella 1 mostra il numero di utenti VPN simultanei che ogni modello di firewall NGFW FortiGate può supportare.

Oltre a garantire la crittografia dei dati in transito tramite VPN, le soluzioni Fortinet offrono una serie di altre funzionalità che possono aiutare un'organizzazione a proteggere la propria forza lavoro remota. Tra queste:

- **Autenticazione a più fattori.** FortiToken e FortiAuthenticator consentono l'autenticazione a due fattori dei dipendenti remoti.
- **Data loss prevention (DLP).** FortiGate e FortiWiFi forniscono la funzionalità DLP per i lavoratori remoti, che è essenziale per i dirigenti che, telelavorando, accedono frequentemente a dati aziendali sensibili.

- **Protezione avanzata dalle minacce.** FortiSandbox analizza il malware e altri contenuti sospetti all'interno di un ambiente sandbox prima che raggiungano la loro destinazione.
- **Connettività wireless.** Gli access point FortiAP garantiscono un accesso wireless sicuro alle postazioni di lavoro remote con gestione completa dell'integrazione e della configurazione da una sola interfaccia.
- **Telefonia.** FortiFone è una soluzione di telefonia VoIP (Voice over IP) sicura, il cui traffico è protetto, gestito e monitorato da un firewall NGFW FortiGate. Disponibile come soft client e in varie versioni hardware.

Modello	Utenti VPN SSL simultanei	Utenti VPN IPsec simultanei	FortiAP gestiti (modalità tunneling)
100E	500	10.000	32
100F	500	16.000	64
300E	5.000	50.000	256
500E	10.000	50.000	256
600E	10.000	50.000	512
1100E	10.000	100.000	2.048
2000E	30.000	100.000	2.048
Tutti i modelli più grandi*	30.000	100.000	2.048
*3300E supporta 1.024 access point in modalità tunneling			

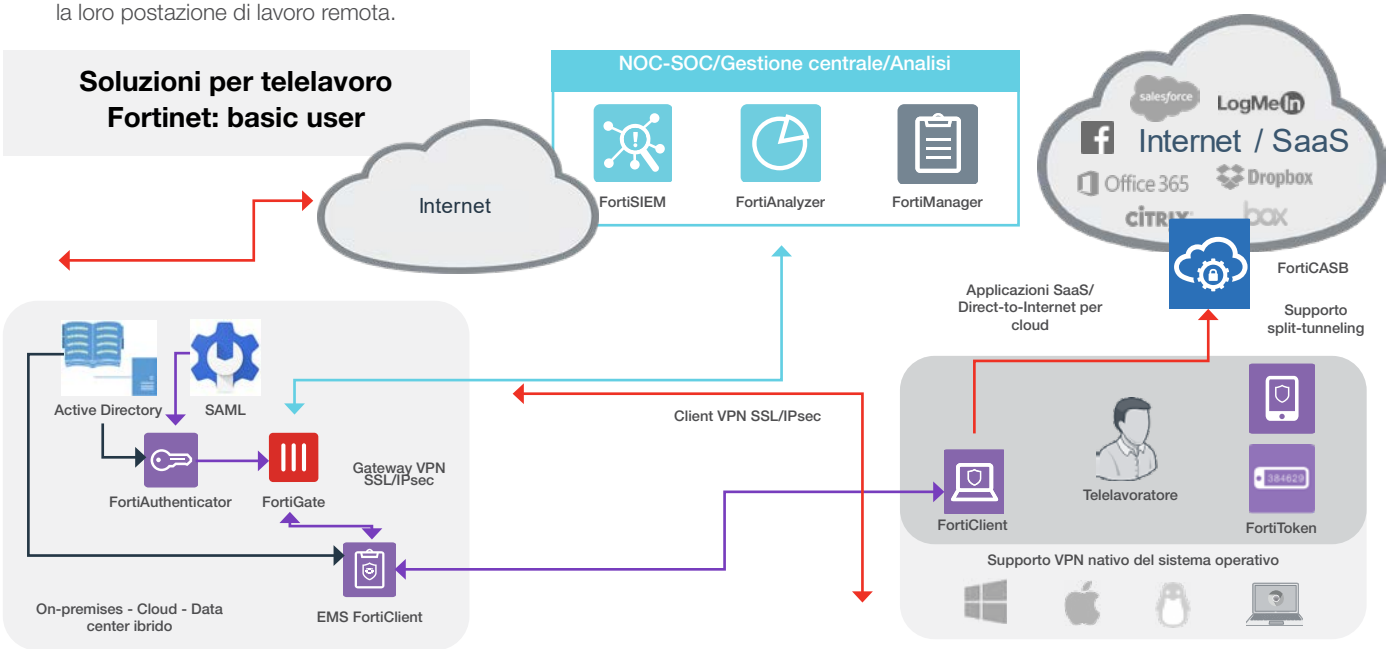
Tabella 1: Numero di connessioni VPN simultanee supportate da vari modelli di firewall NGFW FortiGate.

Casi d'uso dei prodotti Fortinet che supportano il telelavoro

Non tutti i dipendenti di un'organizzazione richiedono lo stesso livello di accesso alle risorse aziendali quando telelavorano. Fortinet fornisce soluzioni di telelavoro su misura per ogni lavoratore remoto:

1. **Basic user** Il basic user necessita solo dell'accesso a e-mail, Internet, teleconferenze, di una condivisione di file limitata e di funzionalità specifiche per lo svolgimento delle sue mansioni (finanze, risorse umane, ecc.) dalla sua postazione di lavoro remota. È previsto l'accesso alle applicazioni Software-as-a-Service (SaaS) nel cloud, come Microsoft Office 365, oltre che una connessione sicura alla rete aziendale.

   I basic user possono connettersi all'organizzazione utilizzando il software client VPN integrato FortiClient e verificare la loro identità con FortiToken per l'autenticazione a più fattori. Si noti che i power user e i super user tornano al profilo basic user nel momento in cui lasciano la loro postazione di lavoro remota.



FortiGate
- Servizi VPN
- Controllo ammissione/conformità
- NGFW
- Fabric Connectors
- Policy dinamica

FortiAuthenticator
- Gestione autenticazione
- Integrazione LDAP/Radius/SAML
- Gestione autenticazione con token/MFA
- Autorità certificazione

EMS (Endpoint Management Server)
- Configurazione client VPN
- Gestione profili/policy endpoint
- Fabric Connector
- Distribuzione FortiClient

FortiClient
- Telemetria endpoint
- Gestione vulnerabilità
- Prevenzione malware
- Web filtering/firewall per applicazioni web
- Supporto VPN/MFA

Figura 1: Distribuzione di una soluzione Fortinet esemplificativa per il basic user.

2. **Power user.** I power user sono dipendenti che richiedono un livello più elevato di accesso alle risorse aziendali quando lavorano da una postazione remota. In ciò può rientrare la capacità di operare in ambienti IT multipli e paralleli (ad esempio, amministratori di sistema, tecnici di supporto IT e personale di emergenza).

   Ai power user, la distribuzione di un access point FortiAP presso la loro postazione di lavoro alternativa garantisce il livello di accesso e sicurezza di cui hanno bisogno. Ciò consente una connettività wireless sicura con tunneling sicuro verso la rete aziendale. Gli access point FortiAP possono essere distribuiti con provisioning zero-touch (ZTP) e saranno gestiti dai firewall NGFW FortiGate in ufficio. Se dovesse essere necessario distribuire un telefono aziendale, può semplicemente collegarsi all'access point FortiAP per la connettività con la sede centrale.

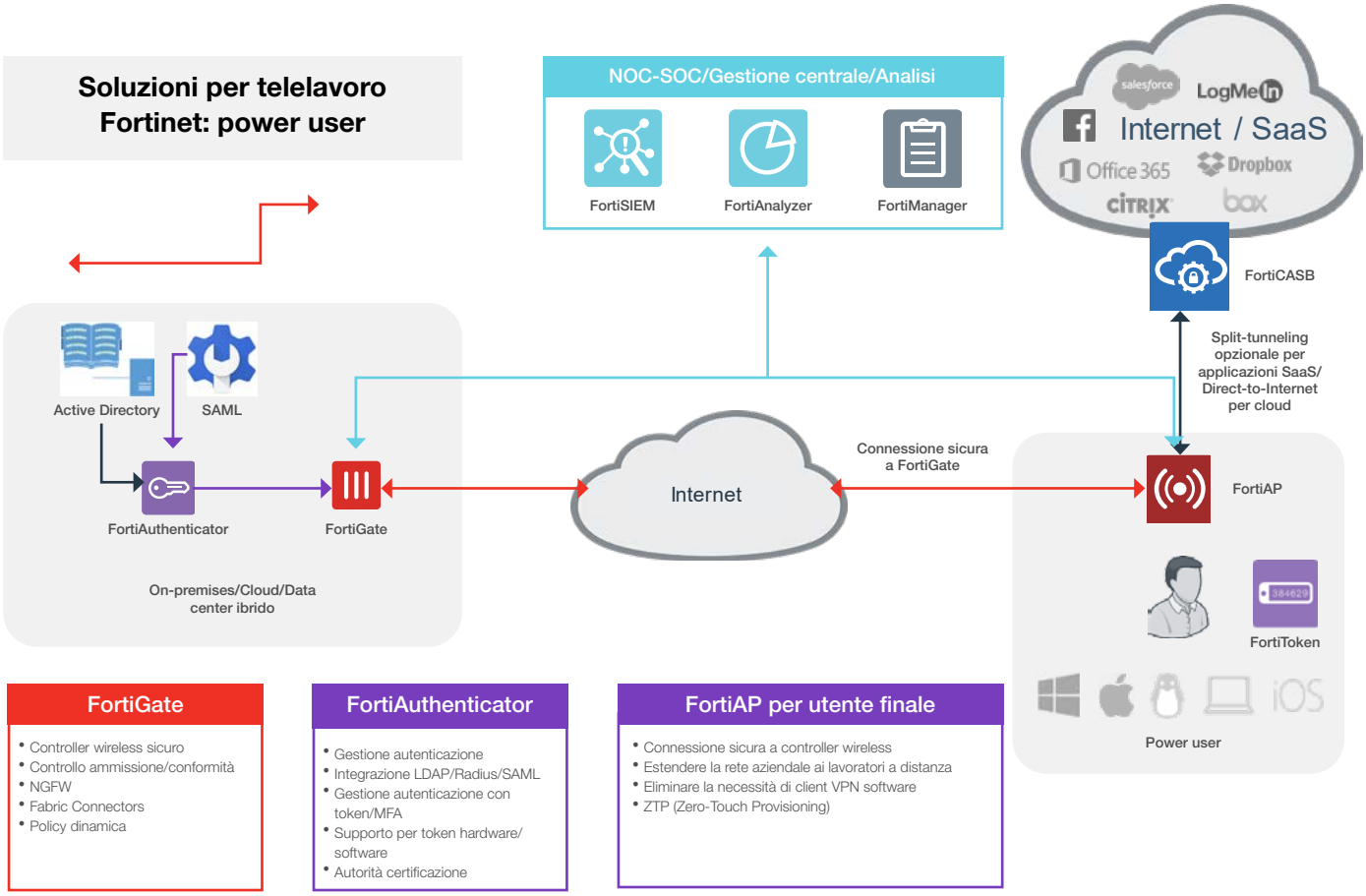


Figura 2: Distribuzione di una soluzione Fortinet esemplificativa per il power user.

3. **Super user.** Un super user è un dipendente che richiede un accesso avanzato a risorse aziendali riservate, anche quando lavora da un ufficio alternativo. Spesso un super user elabora informazioni estremamente sensibili e riservate. Questo profilo di dipendente include amministratori con accesso privilegiato al sistema, tecnici dell'assistenza, partner chiave coinvolti nel piano di business continuity, personale di emergenza e direttori esecutivi.

   Per questi super user, la postazione di lavoro alternativa dovrebbe essere configurata come un ufficio alternativo. Se da un lato servono le stesse soluzioni previste per i basic user e i power user, dall'altro occorrono anche funzionalità aggiuntive. L'access point FortiAP può essere integrato con un firewall NGFW FortiGate o un'appliance FortiWiFi per una connettività wireless sicura con DLP integrato. FortiFone fornisce versioni soft client o hardware di telefonia VoIP gestite e protette tramite firewall NGFW FortiGate in loco o una piattaforma di gestione centralizzata FortiManager distribuita presso la sede centrale.

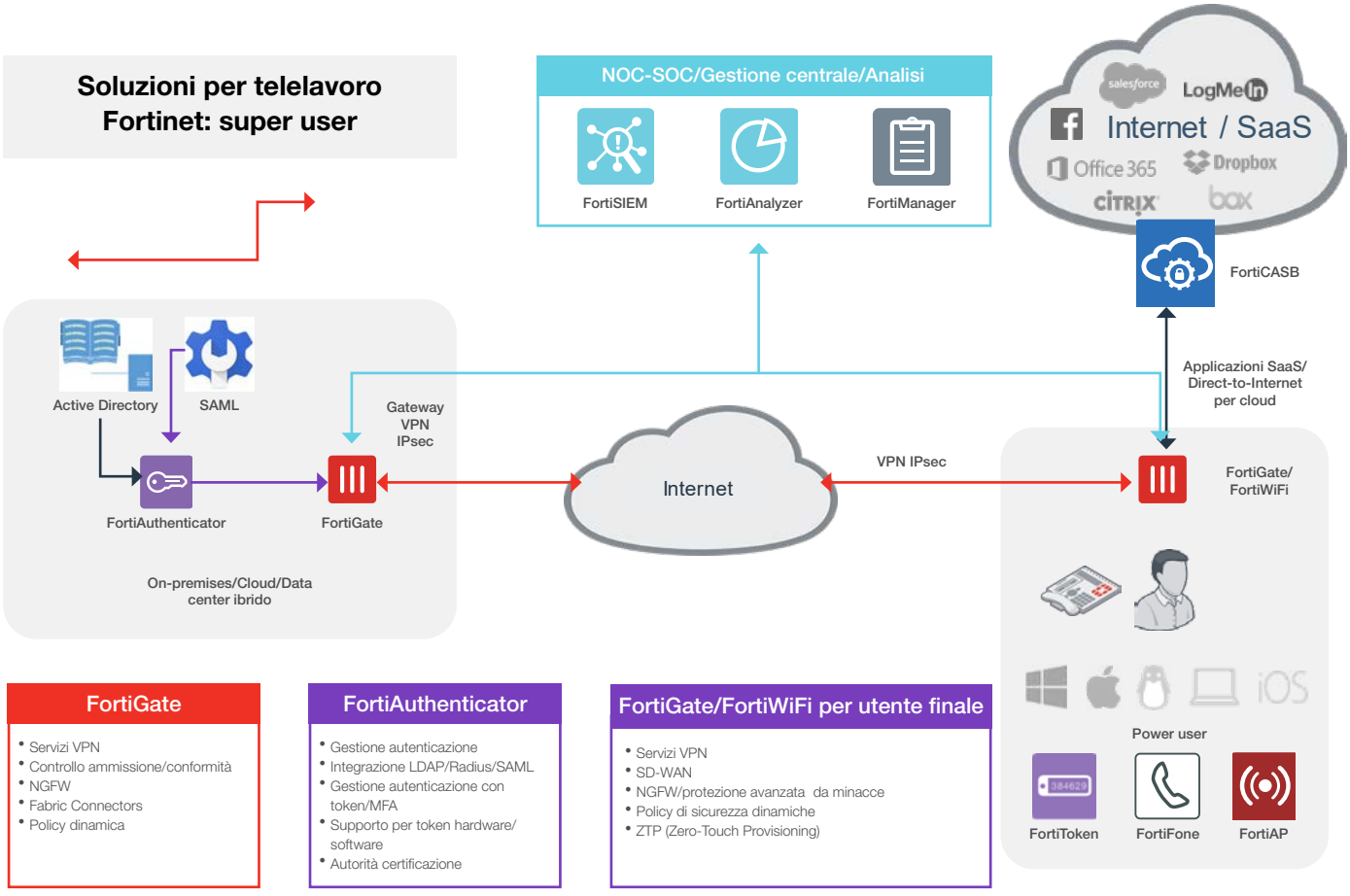


Figura 3: Distribuzione di una soluzione Fortinet esemplificativa per il super user.

A supporto di una forza lavoro remota

Le soluzioni Fortinet sono facilmente distribuibili in postazioni di lavoro remote. Tuttavia, un'organizzazione ha anche bisogno di risorse in loco o nel cloud per supportare in modo sicuro i telelavoratori.

Molte organizzazioni già dispongono di queste risorse in quanto fanno parte della loro architettura di sicurezza esistente. Un NGFW FortiGate fornisce un firewall in grado di ispezionare il traffico crittografato e in chiaro su scala aziendale con un impatto minimo sulle prestazioni, ma include anche un gateway VPN integrato che funge da endpoint per le connessioni crittografate ai telelavoratori.

Il firewall NGFW FortiGate prevede anche l'integrazione con l'infrastruttura IT comune, compresi i servizi di direzione aziendale, come Microsoft Active Directory (AD), e le soluzioni MFA e single sign-on (SSO). FortiAuthenticator fornisce un unico punto di integrazione centralizzato per le soluzioni di autenticazione e supporta soluzioni di terzi, così come FortiToken, che offre opzioni hardware, software, e-mail e mobile token.

Quando si gestisce una forza lavoro remota e distribuita, la visibilità e la gestione della sicurezza centralizzate sono essenziali. Tutte le soluzioni Fortinet possono essere integrate tramite il Fortinet Security Fabric. Ciò consente al team di sicurezza dell'organizzazione di ottenere visibilità e controllo da un'unica interfaccia con FortiManager, eseguire l'aggregazione dei log e l'analisi della sicurezza con FortiAnalyzer, nonché rilevare e rispondere rapidamente a potenziali minacce con FortiSIEM.

Ottenere la piena integrazione della sicurezza con le soluzioni Fortinet

Il Fortinet Security Fabric consente una perfetta integrazione della forza lavoro remota di un'organizzazione. Tutte le soluzioni Fortinet sono collegate tramite il Fortinet Security Fabric, che consente visibilità, configurazione e monitoraggio tramite un'unica interfaccia. Una serie di Fabric Connectors, un ambiente API aperto, il supporto della comunità DevOps e un ampio ecosistema Security Fabric esteso permettono l'integrazione con oltre 250 soluzioni di terzi.

Questo è essenziale quando un'organizzazione sta approntando un piano di business continuity poiché l'azienda potrebbe essere costretta a passare a una forza lavoro completamente remota con poco o nessun preavviso. La visibilità e la gestione da un'unica interfaccia dell'architettura di sicurezza di un'organizzazione assicura che il supporto del telelavoro non metta a rischio la sicurezza informatica dell'organizzazione.

Le seguenti soluzioni fanno parte del Fortinet Security Fabric e supportano un telelavoro sicuro:

- **FortiClient.** FortiClient rafforza la sicurezza degli endpoint attraverso l'integrazione di visibilità, controllo e difesa proattiva, consentendo alle organizzazioni di individuare, monitorare e valutare i rischi degli endpoint in tempo reale.
- **FortiGate.** I firewall NGFW FortiGate utilizzano processori di sicurezza informatica appositamente realizzati per garantire la massima protezione, la visibilità end-to-end e il controllo centralizzato, oltre all'ispezione ad alte prestazioni del traffico in chiaro e crittografato.
- **FortiWiFi.** I gateway wireless FortiWiFi abbinano i vantaggi di sicurezza dei firewall NGFW FortiGate a un punto di accesso wireless, fornendo una soluzione di rete e sicurezza integrata per i telelavoratori.
- **FortiFone.** FortiFone garantisce comunicazioni vocali unificate con connettività VoIP protetta e gestita tramite firewall NGFW FortiGate. L'interfaccia del soft client FortiFone permette agli utenti di effettuare o ricevere chiamate, accedere alla segreteria telefonica, controllare la cronologia delle chiamate e cercare nell'elenco dei contatti dell'organizzazione direttamente da un dispositivo mobile. Sono disponibili diverse opzioni hardware.
- **FortiToken.** FortiToken conferma l'identità degli utenti aggiungendo un secondo fattore al processo di autenticazione attraverso token basati su dispositivi fisici o app mobili.
- **FortiAuthenticator.** FortiAuthenticator fornisce servizi di autenticazione centralizzata, compresi servizi SSO, gestione dei certificati e gestione degli ospiti.
- **FortiAP.** FortiAP offre un accesso sicuro e wireless alle imprese distribuite e ai lavoratori remoti e può essere facilmente gestito da un firewall NGFW FortiGate o tramite cloud.
- **FortiManager.** FortiManager fornisce un'unica interfaccia di gestione e controllo delle policy in tutta l'azienda estesa per analizzare le minacce basate sul traffico a livello di rete. Ciò include funzionalità per contenere gli attacchi avanzati e la scalabilità per gestire fino a 10.000 dispositivi Fortinet.
- **FortiAnalyzer.** FortiAnalyzer garantisce la sicurezza informativa e la gestione dei log sulla base dell'analisi per consentire un migliore rilevamento delle minacce e una maggiore prevenzione delle violazioni.
- **FortiSandbox.** Le soluzioni di sandboxing proposte da Fortinet offrono una potente combinazione tra rilevamento avanzato, mitigazione automatizzata, informazioni utili all'azione e distribuzione flessibile per bloccare gli attacchi mirati e la conseguente perdita di dati. Disponibile come servizio cloud incluso nella maggior parte degli abbonamenti FortiGuard.

Una base sicura a garanzia della continuità operativa

Approntare un piano di business continuity e disaster recovery è vitale per qualsiasi organizzazione. Una sua componente importante è la capacità di supportare una forza lavoro in gran parte o completamente remota con poco o nessun preavviso.

Quando si sviluppano piani di business continuity, è essenziale assicurarsi che l'organizzazione disponga delle risorse necessarie per proteggere la forza lavoro remota. Le soluzioni Fortinet, facilmente distribuibili e configurabili, permettono all'organizzazione di mantenere pienamente sicurezza, visibilità e controllo, a prescindere dall'ambiente di distribuzione.

1 "The Benefits of Working From Home," Airtasker, 9 settembre 2019.

2 Ibid.

3 Abdullahi Muhammed, "Here's Why Remote Workers Are More Productive Than In-House Teams," Forbes, 21 maggio 2019.

4 Ibid.

maggio 11, 2020 12:40 PM

618770-0-1-IT

C:\Users\marcel.kotkowski\Downloads\Fortinet\P-356016\06_wf\Work\sb-FA-secure-remote-access-for-your-workforce-at-scale-3132020_A4